(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 November 2001 (29.11.2001)

PCT

(10) International Publication Number
WO 01/91369 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/CA01/00725

(22) International Filing Date: 22 May 2001 (22.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/205,562 22 May 2000 (22.05.2000) US

(71) Applicant *(for all designated States except US)*: **ORCHESTREAM CANADA CORPORATION** [CA/CA]; 350 Terry Fox Drive, Kanata, Ontario K2K 2W5 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **FALLAH-KHAIR, Melody** [CA/CA]; 5 Cheltonia Way, Kanata, Ontario K2T 1G1 (CA). **SOMJI, Arif** [CA/CA]; 350 Terry Fox Drive, Kanata, Ontario K2K 2W7 (CA).

(74) Agent: **MITCHELL, Richard, J.**; c/o Marks & Clerk, P.O. Box 957, Station B, Ottawa, Ontario K1P 5S7 (CA).

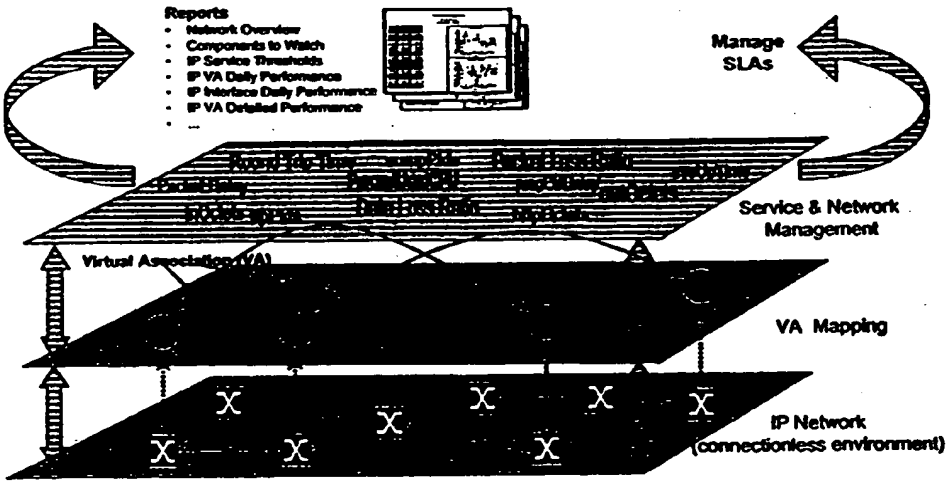
(81) Designated States *(national)*: CA, DE, GB, SE, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD OF MODELING A DIGITAL COMMUNICATIONS NETWORK



(57) Abstract: A domain/object model of a packet-switched digital communications network contains devices, data collection, and services as separate entities. The domain/object model provides explicit representation of key objects, and key service and network performance metrics.

WO 01/91369 A2

METHOD OF MODELING A DIGITAL COMMUNICATIONS NETWORK

Field of the Invention

This invention relates to the field of digital communications networks, and in particular to a method of modeling objects in such networks. The invention is applicable to IP networks, such as the Internet.

Background Of The Invention

The inherently unpredictable nature of IP networks coupled with the explosive demand for IP based services and the ever increasing e-commerce economy in which we live has highlighted the need for reliable, assured, quality IP Network and Services. For the service provider this means fully understanding their IP networks both at the network and service level. An important part of this understanding is the ability to know how specific parts of the network are performing. An object of the invention is to meet this need.

Summary of the Invention

According to the present invention there is provided a domain/object model of a packet-switched digital communications network that contains devices, data collection, and services as separate entities, wherein said domain/object model provides explicit representation of key objects, and key service and network performance metrics.

The packet switched network is typically an IP network. The model preferably includes the modeling of various types of Systems and Interfaces along with Virtual Associations (VA). Virtual Associations offer an ability to virtually "link" two points in an IP network, allow for performance measurements to be collected and analyzed for this virtual association. Virtual Associations give service providers logical views into their IP networks, instead of viewing the environment as a compilation of unrelated routers and devices. Virtual Associations take network and service assurance and performance management to the next level in an IP environment. The ability to have a logical "connection" oriented view within an inherently connectionless environment sheds light on what has been an unpredictable and unreliable networking environment. The Virtual Associations give service providers logical views into their IP networks, instead of viewing the environment as a compilation of unrelated routers and devices.

The model for IP objects may be integrated with the object models for management of other network technologies, including Frame Relay, ATM and TDM. This allows integrated analysis of performance across heterogeneous networks, for both network and service level objects. The architectural flexibility of the object model is important as the network and services change over time. This flexibility provides the ability to add new devices into the model as needed, and add new measurement metrics to objects as needed.

The IP domain modeling provides an open system, able to be selective about the specific objects and information that are to be monitored. The model provides a basis for enhanced reporting on IP based objects, for network and service reporting, and forms the basis for performance reporting on IP VPNs. In the model, systems are modeled as Network Access Layer Systems (e.g. Repeater, Bridge, L2 switch); Network Layer Systems (L3 devices such as routers; e.g. Cisco, 3com, Bay routers); End-to-End System (servers, hosts, printers); and Application Layer Systems (FTP client/FTP server, SMTP client/SMTP server). Interfaces are physical or logical traffic carrying entities (e.g. interface ports).

The invention is particularly suited for use with Orchestream Corporations Resolve™ network management software.

In another aspect the invention provides a method of modeling a network to provide information pertaining to the operation of the network, comprising establishing virtual associations between at least two points on the network whereby performance measurements can be collected and analyzed for each virtual association.

Brief Description of the Drawings

The invention will now be described in more detail, by way of example only, with reference to the accompanying drawings, in which:-

Figure 1 is a diagram of an IP network showing virtual associations;

Figure 2 is a diagram of a web-hosting server;

Figure 3 shows an end point analysis;

Figure 4 shows an IP_VPN scenario;

Figure 5 shows and example of a secure IP_VPN;

Figure 6 shows an example of a MPLS (LSP); and

Figure 7 shows an OSS integration.

Detailed Description o the Invention

In order to understand the invention, it is important to understand the concept of virtual associations (Vas) implemented in the model. Figure 1 illustrates a network topology modeled using Virtual associations (VAs) in accordance with the principles of the invention. VAs provide a mechanism to model and assess performance between two associated entities in a connection-less network environment. They are uni-directional and can be configured by the end-user.

The end-points of a VA are known as Virtual Association Termination Points (VATPs). A VATP is a virtual identifier for identifying each end-point of a Virtual-Association. A Virtual Identifier is typically the IP-address of the end-point being measured: a sole IP Address on an interface, an Interface's IP-address, a Transport Address (IP Address + port), or a System's IP-address. The end-points used to form VATPs are synced from external sources, e.g. a Resolve SNMP Data Manager or an NMS.

The VAs are the IP-addresses of the end-point to be measured (e.g. port, interface, system.). VAs are configurable (through the Resolve Configurator. VAs may also be configured for mass-importation via CrossKeys Professional), allowing the user to acquire information on specific areas of the network, while having the ability to set performance thresholds to monitor service levels, and network trends. Virtual Associations are based on how service providers deploy their services. They may be configured within a Point-Of-Presence (POP) or between POPs. They form the basis of hot spotting, tying in or associating two management points to facilitate the performance analysis of IP-based services.

VAs can be used to measure packet loss, latency, reachability, protocol distribution, as well as, bytes and packets per protocol to track daily, monthly, and detailed performance between two points in the network for network performance reporting. These parameters are then tied to configurable IP service thresholds, based on the customer's defined SLAs, for analysis of violation trends for service performance reporting on a daily and monthly basis.

Virtual Associations are appropriate for long and short term associations. Long-term associations could be for monitoring site-interconnections. Short-term associations could be for monitoring tunnels for VPN remote access.

The network shown in Figure 1 has pairs of switches X linked through virtual associations. The VAs allow for performance measurements to be collected and analyzed for each virtual association.

The Virtual Association concept is intrinsically linked to the IP domain model. The domain model that contains devices, data collection, and services as separate entities. These can be added or removed to model the service provider's network and service environment. The domain model provides explicit representation of key IP objects. This includes the modeling of various types of Systems and Interfaces along with theVirtual Associations (VA).

The model for IP objects can be integrated with the object models for management of other network technologies, including Frame Relay, ATM and TDM. This allows integrated analysis of performance across heterogeneous networks, for both network and service level objects. The architected flexibility of the object model is important as the network and services change over time. This flexibility provides the ability to add new devices into the model as needed, and add new measurement metrics to objects as needed.

The IP domain modeling provides an open system, able to be selective about the specific objects and information that are to be monitored. The model provides a basis for enhanced reporting on IP-based objects, for network and service reporting, and forms the basis for performance reporting on IP-VPNs.

In the IP domain model systems are modeled as Network Access Layer Systems (e.g. Repeater, Bridge, L2 switch); Network Layer Systems (L3 devices such as routers; e.g. Cisco, 3com, Bay routers); End-to-End System (servers, hosts, printers); and Application Layer Systems (FTP client/FTP server, SMTP client/SMTP server).

Interfaces are physical or logical traffic carrying entities (e.g. interface ports)

The VAs then provide a mechanism to model and assess performance between two associated entities in a connection-less network environment. They are uni-directional and can be configured by the end-user. The end-points of a VA are known as Virtual

Association Termination Points (VATPs). These are the IP-addresses of the end-point to be measured (e.g. port, interface, system.). VAs are configurable , allowing the user to acquire information on specific areas of the network, while having the ability to set performance thresholds to monitor service levels, and network trends. Virtual Associations are based on how service providers deploy their services. They may be configured within a Point-Of-Presence (POP) or between POPs. They form the basis of hot spotting, tying in or associating two management points to facilitate the performance analysis of IP-based services.

VAs can be used to measure packet loss, latency, reachability, protocol distribution, as well as, bytes and packets per protocol to track daily, monthly, and detailed performance between two points in the network for network performance reporting. These parameters are then tied to configurable IP service thresholds, based on the customer's defined SLAs, for analysis of violation trends for service performance reporting on a daily and monthly basis.

Virtual Associations are appropriate for long and short term associations. Long-term associations could be for monitoring site-interconnections. Short-term associations could be for monitoring tunnels for VPN remote access.

Available reports are useful for Account Managers, Service Representatives as well as Engineering (Network Planning and Operations).

Sample Scenario: Dedicated Web-Hosting/Application/Server (See Figure 2)

As service providers deploy web hosting services for their customers, the quality of experience that the end user (web surfer, customer) experience in using and accessing the web site becomes of critical importance. Enterprises that outsource this important business tool demand service assurance in the form of meaningful SLAs from their providers.

A user wishes to assess network and service performance for a web-hosting application that is running on a dedicated web-server or host at a Point of Presence (POP). By configuring a VA, the service provider can determine performance information of the VA that models the web hosting service. By focusing on a slice of the overall network, the VA, the service provider can monitor network performance and assess specific network

quality indices. At the service level, the service provider can look at service thresholds, violations, trends and other indicators of quality of service. This can be achieved by configuration of a Virtual Association, setting service performance thresholds on the VA, and analyzing the network and service performance for the given VA.

From Virtual Association analysis, the user can assess performance of the end-points of the configured VA -look at the end-point that has the web-server running on it, and compare that interface's performance to other interfaces in the network. Each interface can then be compared in aggregate to the performance of systems (that would have several other interfaces on them).

Through the Resolve Configurator GUI, a user configures a VA from the POP to the web-hosting server (see Appendix for details on creating a VA from the GUI). The user sets appropriate threshold levels for VAs' reporting, and commits (saves) the VA(s). Thresholds are for Average Round-Trip-Time (ie. service latency) and Reachability.

The user tracks network and service performance by looking at data on various reports as follows: From the Network Overview Report showing overall performance of IP, as well as, FR and ATM, the user hones in on latency for the configured VAs by drilling-down to the Key Performance Indicator Report to assess trend of the VA.

Also from the Network Overview, the user decides to drills-down to the Violation Trend Report that lists all network performance violations based on user-set thresholds for Systems, Interfaces, and VAs. From this, the user gets an idea of the VA's daily and monthly performance for Reachability, Availability, Outage Counts, Outage Seconds, Average Round Trip Transfer Time (Average RTT or average latency) .

Additionally, from the Network Overview, the user wishes to find out a detailed list of all violations including those for the configured VA(s) by looking at the aggregateViolation List Report . The user also wishes to find out details of service as well as network violations specific to the configured VA. For network-level violations, the user drills down to the Components to Watch. To assess service-level violations, the user drills down to detailed views of, Services to Watch , and IP service Thresholds.

The user now wishes to see daily performance of the configured VA(s) to identify details on usage, track traffic patterns (protocol distributions), determine delay, loss and

reachability patterns for the configured VA(s), and thus the web-hosting service. From either of the network and service views above, the user drills-down to the IP VA Daily Performance Reports as well as IP VA Detailed Performance Reports that show charts on Loss, Latency, Reachability, and Bytes per Protocol, and Packets Per Protocol .

From the above analyses, the user is able to track the network and service performance of the VA. He is able to see and monitor network performance of the web-hosting site and assess specific network quality indices through the configured VA. He is able to see and monitor the service thresholds, violations, trends and indicators of quality of service for the web-hosting site through the configured VA. He is able to compare the performance of the server site to that of other areas in the network as follows.

From the analysis of VAs, the user now wishes to assess performance of the end-points of the configured VA -look at the end-point that has the web-server running on it, and compare that interface's performance to other interfaces in the network. In turn, the user wishes to then compare the performance of these interfaces, in aggregate, to the performance of systems (which may have several interfaces on them). To do this, from the IP VA Daily Performance, the user drills across to the IP Interfaces Daily Performance Reports , and to the IP Systems Performance Reports.

From Virtual Association analysis, the user is able to then assess performance of the end-points of the configured VA, look at the end-point that has the web-server running on it, and compare that interface's performance to other interfaces in the network (see Figure 3). The user can gain insight on the performance of the VA's end-point interface to those of other interfaces in the POP (POP1). Furthermore, the user can see network and service level performance of these interfaces to other systems' interfaces in the network (POP2 & POP3) and look at network and service performance of the systems as well throughout the entire network.

In the above analysis, the user can go directly to detailed reports from earlier steps. The above detailed scenarios are meant to capture a full-breadth and in-depth analysis. In addition, he user can create other types of reports tailored to his/her specific needs, and attach them as drill-throughs to reports identified in any of the scenarios above.

Sample Scenario: CrossKeys Resolve Virtual Associations in the context of IP VPNs

Below (see Figure 4) is a description of how Virtual Associations can improve the performance of an IP based VPN service, which provides a set of IP Services including Internet Access, Dial Up connectivity and site to site IP data transmission.

Virtual Associations can be configured by the user so that "hot spots" or segments of the IP VPN service are modeled as VAs. The multiple VAs that comprise the service can then be reported on individually (per VA), collectively (as a whole IP VPN service) and/or by interface and system of which each VA is derived from. The end result is a clear picture of the IP VPN service and it's performance.

From the Figure 4, it will be seen that the IP VPN's performance as a whole entity (as defined by the VAs) and each segment of the IP VPN – Remote dial access performance, dedicated internet access points, site-interconnect performance are all measured, monitored, and reported on.

VA 1, which is configured to map onto the dial service can include the Remote Access Server (RAS) as one VATP and the Edge VPN Router (POP 1) as the other VATP. The first VATP, is the fixed ingress (network-facing) port of the Remote Access Server that interfaces onto the service provider's IP network. The second VATP is an interface on the service provider's router POP 1. From this VA, performance of this dial-in segment can be measured and monitored.

VA 2, which is configured from the router (POP 2) as one VATP to the edge router on the customer's main site (CPE 1) which acts as the VA 2's VATP. Monitoring this VA would give the service provider performance information on the primary IP VPN link into the service provider's IP network cloud from the enterprise's main or critical site.

VA 3, which is configured from the customer's router (CPE 2) to the service provider's nearest POP (POP 3) models the dedicated IP VPN access offered by the service provider to that end customer. This VA would collect and show performance reporting for this segment of the IP VPN service.

VA 4, VA 5 and VA 6 are each configured to include 2 major POPs within each VA. This is done to monitor the backbone performance of the IP VPN.

VA 7 is monitoring the performance of a "permanent" VPN or site interconnect, created between a router/server at the corporate head quarters (main IP VPN site CPE 1) and the router/server at the branch office (CPE 3).

All together, these VAs can model an IP VPN service and thus enable the service provider to gain insight as to the performance of this IP VPN service as a holistic service offering, and or by segment, customer or device included within the configured IP VPN service. This flexibility and ability to model the service in different views (network, service, per customer) is unique to CrossKeys Resolve. The power and value of Virtual Association modeling is evident in this scenario.

Sample Scenario: Monitoring the Performance of an Enterprise's secure (encrypted) IP VPN connection (Figure 5)

- Each corporate user's PC client is security enabled with encryption software residing on the PC.
- The corporate user dials into a local public POP and is authenticated on that RAS to access the Internet.
- The user is then authenticated at their corporate site (fixed IP Address) for the secure Internet tunnel to be established.

By configuring and using VAs in this scenario, the same benefits apply as in the IP VPN dial in example in the section above. Creating and monitoring the performance of VAs: between customer sites, between a customer site and a Network Access Point (NAP), between a POP and the customer site, and also between POPs gives the service provider the ability to measure, monitor and report on performance for a secure IP VPN service.

Sample Scenario: VAs Used to Represent MPLS Label Switched Paths (Figure 6)

The system gives services providers the ability to measure and analyze the performance of new and emerging networking standards like MPLS and DiffServ.

With MPLS, where label switched paths exist by having been created autonomously in the network, and/or having been created by external management (creation and status reporting through traps/notification), VAs can be used to map label switched paths to

monitor overall performance and assess the effectiveness of the MPLS-engineered network .

Sample Scenario: Intelligent Discovery by Application in or Adjacent to Resolve (Figure 7)

Network usage and traffic data is used to identify network flows. Virtual Associations may be used in the following manner to assess network usage and traffic data used to identify network flows.

An Adjunct application (such as a Flow Analyzer in the above diagram) identifies flows and flow data between points by applying analysis techniques to Resolve's performance data.

The traffic flow-patterns between 2 network points are modeled as VAs within the network management system.

The system acquires and summarizes flow data.

The created VAs can then be related to overall network and service performance.

The identified scenario would be useful for network planning and engineering, as well as, customer account management. Some examples of how this application could be applied are:

- network prediction - flow prediction allows for effective engineering of the network and thus enhanced quality of service
- capacity forecasting - allows for "what-if" scenarios to see how new IP-based services effect, or will effect, the service provider network
- know when to build out network - allows service providers to predict when they require additional networking infrastructure to account for new, yet-to-be deployed services, or to meet growing demands on existing services
- optimizing network design - allows for optimizing of already-deployed network resources

For the service provider, virtual Associations are a means of gaining control over their IP networks. They allow for the optimizing of infrastructure investments, streamlining of OSS processes, and knowing what is happening both at the network and service level in an aggregated manner. Using the system's reporting capabilities, users are able to develop their own custom reports as well. In addition, these reports may be attached as drill-throughs to existing reports.

If the association between two IP interfaces is not defined in the sources NMS, it must be configured in Resolve before Resolve can monitor the interface to interface performance. Because a virtual association represents only one direction of traffic, associating two IP interfaces creates two virtual associations.

Flow of Events

The following steps describe how to set up virtual associations through the Resolve Configurator:

1. The User. opens a new Virtual Association detail window.
   The User. opens a Component lookup to search for the first IP interface.
   The User. enters search filter criteria and clicks "Search". (The filter criteria are system name, interface name and source NMS.)
   The system lists the interfaces that match the search criteria.
   The User. selects the components that are used to provide this service and clicks "OK".
2. The system adds the selected components to the Virtual Association detail window.
   The User. repeats steps 2 to 6 for the second IP interface.
   The system displays the default VA names based on the interface names.
   The User. types in new VA names (OPTIONAL).
   The User. saves the VA definitions.
   The system saves the VA definitions to the database (Resolve Service Management Information Base -SMIB).

Pre-Conditions

The targets (ie. IP port, interface, system, addresses) of the VA's VATPs must exist in the Resolve database. These are synced (ie. inhaled) from external sources, e.g. a Resolve SNMP Data Manager or an NMS.

Post-Conditions

The New Virtual Association is created in the database

Some possible applications of the system described are as follows:

Monitoring the Performance of ISP Peering Points Interconnection.

Choose two routers in each peering points, one as source and one as destination.

- Configure the Routers to perform the ICMP Echo (Ping) between the two sites.
- Create a Virtual Association (VA) between two routers in each peering point (NAP) using the IP Addresses.
- Resolve collect the data through PVM and summarize it.
- Monitor the performance of the VA by generating Reports at the Resolve Ni level :
  - Availability
  - reachability
  - PLR

Monitoring the Performance of an Enterprise Network (Star Topology).

- Choose a router in the Headquarter and one in each branch office.
- Configure the Routers to perform the ICMP Echo (Ping) between either the branch office to headquarter or vice versa.
- Create a Virtual Association (VA) between each two routers in each peering point (NAP) using their IP Addresses.
- Resolve collect the data through PVM and summarize it.
- Monitor the performance of the VA by generating Reports at the Resolve Ni level :
  - Availability
  - reachability
  - PLR

Monitoring the Performance of Internet Connection.

- By creating and monitoring the performance of VA :
  - o between customer sites
  - o between a customer site and a NAP
  - o between a POP and a customer site
  - o between POPs used by the customer.

Monitoring the Performance of the backbone link.

- By creating and monitoring the performance of VA : between two routers at each end of the link

Monitoring the Performance of a Permanent VPN.

- By creating and monitoring the performance of a service with Virtual Accociations : created between a router/server at the headquarter of the P-VPN and a router/server at each branch office.

It will be appreciated from the above-described examples that the use of virtual associations in a network management environment provides an efficient way to monitor the performance of segments of a network.

Claims:

1. A domain/object model of a packet-switched digital communications network that contains devices, data collection, and services as separate entities, wherein said domain/object model provides explicit representation of key objects, and key service and network performance metrics.

2. A domain/object model as claimed in claim 1, wherein a plurality of points on a network a logically linked through virtual associations.

3. A domain/object model as claimed in claim 2, wherein said virtual associations are identified by identifiers associated with endpoints of the association.

4. A domain/object model as claimed in claim 3, wherein said network is an IP network.

5. A domain/object model as claimed in claim 4, wherein said identifiers are the IP addresses of the endpoints.

6. A method of modeling a network to provide information pertaining to the operation of the network, comprising establishing virtual associations between at least two points on the network whereby performance measurements can be collected and analyzed for each virtual association.

7. A method as claimed in claim 6, wherein said virtual associations are identified by identifiers associated with the endpoints thereof.

8. A method as claimed in claim 6, wherein said network is an IP network and said identifiers comprises the IP addresses of the endpoints associated with the virtual connections.

9. A method as claimed in claim 6, wherein said virtual associations are used measure parameters for tracking daily, monthly, and detailed performance between two points in the network for network performance reporting.

10. A method as claimed in claim 9, wherein said virtual associations are used to measure packet loss, latency, reachability, protocol distribution, bytes and packets per protocol.

11. A method as claimed in claim 9, wherein said parameters are then tied to configurable IP service thresholds, based on the customer's defined service level agreements for analysis of violation trends for service performance reporting on a periodic basis.

12. A method as claimed in claim 6, wherein said virtual associations are associated with specific network services to permit the monitoring of said specific services.

13. A method as claimed in claim 7, wherein one said endpoint is a local server and another said endpoint is a remote server.

14. A method as claimed in claim 6, wherein said virtual associations are used to monitor virtual private network tunnels.

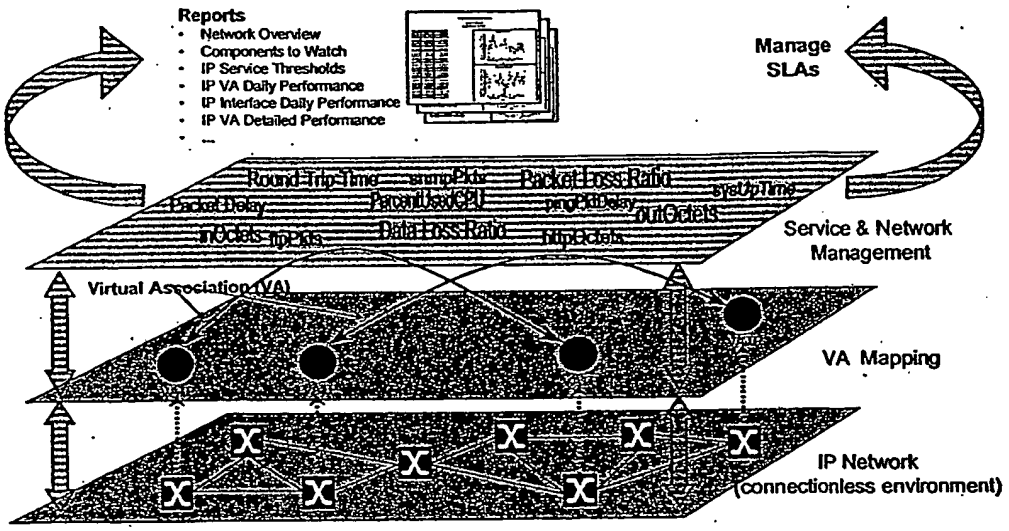


Figure 1

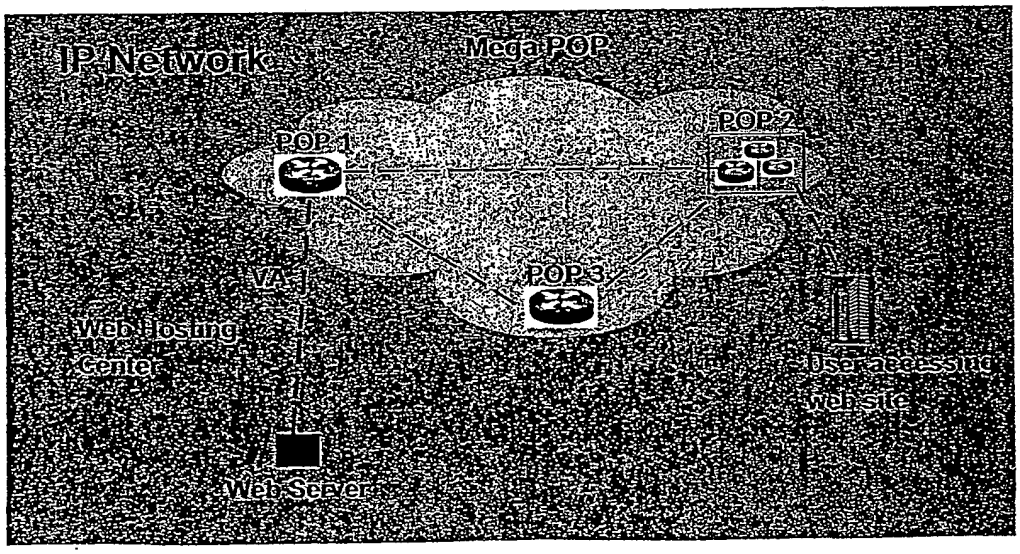


Figure 2

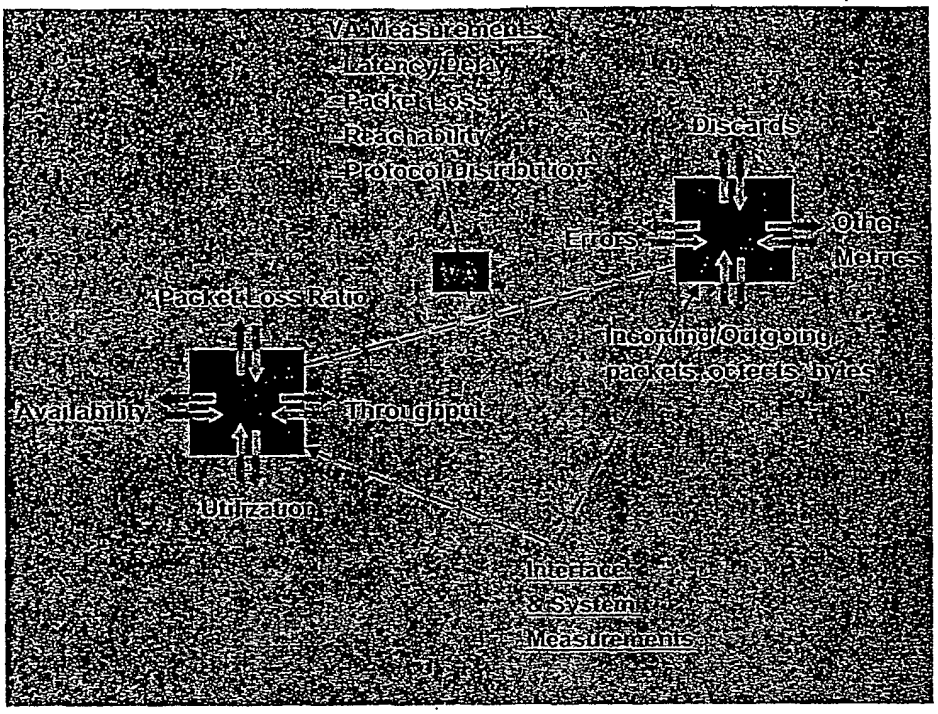


Figure 3

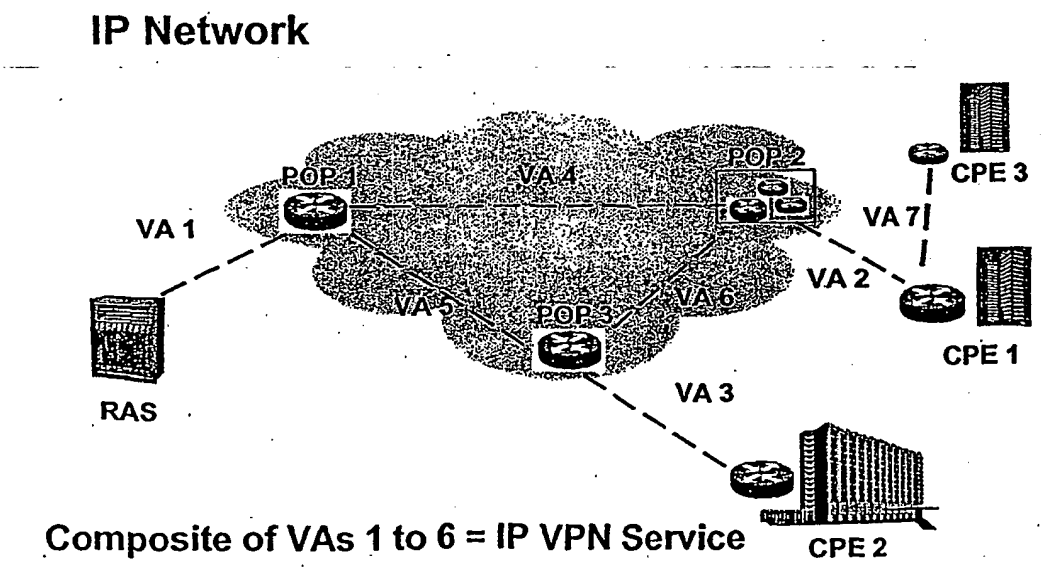


Figure 4

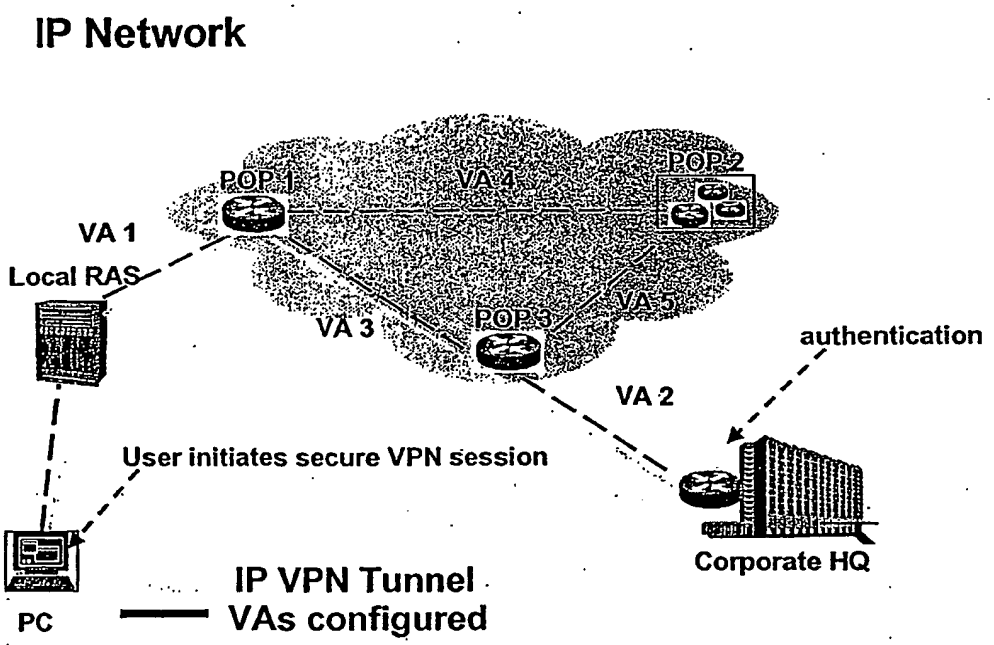


Figure 5

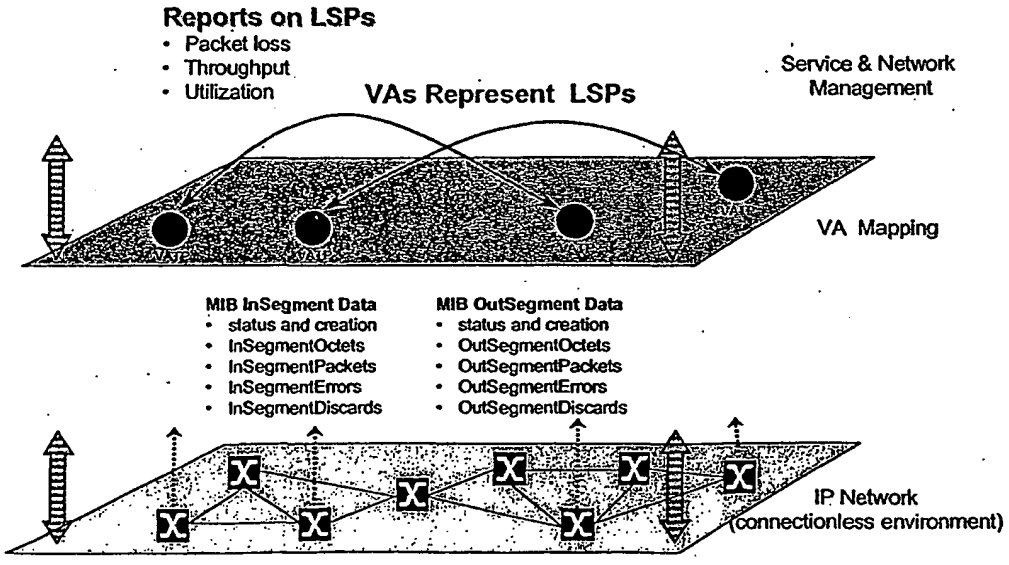


Figure 6

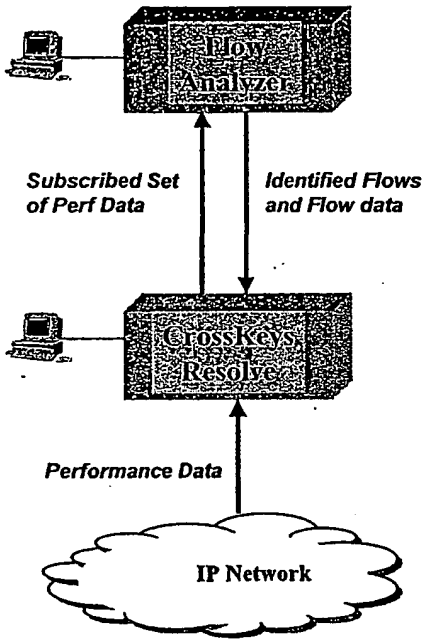

Flow Analyzer
Subscribed Set of Perf Data
Identified Flows and Flow data
CrossKeys Resolve
Performance Data
IP Network

Figure 7

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 November 2001 (29.11.2001)

PCT

(10) International Publication Number
WO 01/091369 A3

(51) International Patent Classification[7]: H04L 12/26, 12/24

(21) International Application Number: PCT/CA01/00725

(22) International Filing Date: 22 May 2001 (22.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/205,562 22 May 2000 (22.05.2000) US

(71) Applicant *(for all designated States except US)*: **ORCHESTREAM CANADA CORPORATION** [CA/CA]; 350 Terry Fox Drive, Kanata, Ontario K2K 2W5 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FALLAH-KHAIR, Melody** [CA/CA]; 5 Cheltonia Way, Kanata, Ontario K2T 1G1 (CA). **SOMJI, Arif** [CA/CA]; 350 Terry Fox Drive, Kanata, Ontario K2K 2W7 (CA).

(74) Agent: **MITCHELL, Richard, J.**; c/o Marks & Clerk, P.O. Box 957, Station B, Ottawa, Ontario K1P 5S7 (CA).

(81) Designated States *(national)*: CA, DE, GB, SE, US.

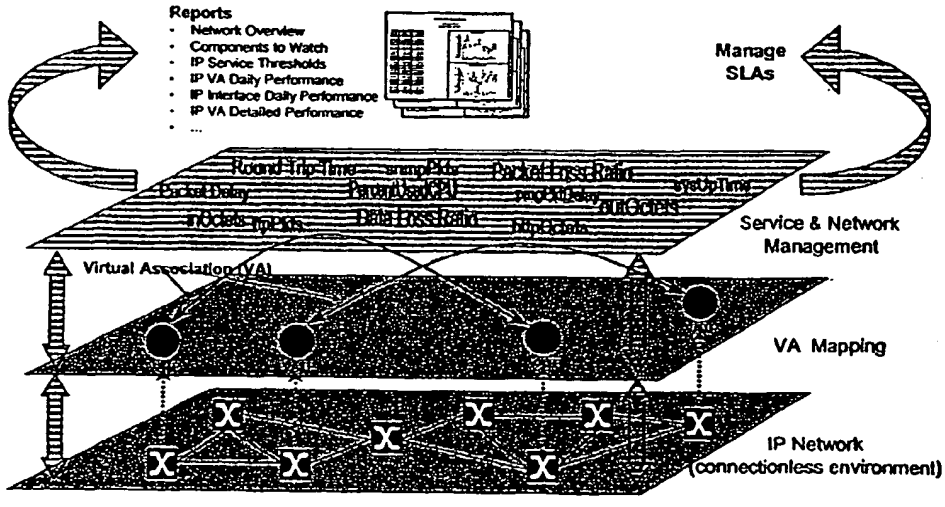
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

(88) Date of publication of the international search report:
1 August 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: OBJECT ORIENTED MANAGEMENT OF SERVICES AND AN IP-NETWORK



(57) Abstract: A domain/object model of a packet-switched digital communications network contains devices, data collection, and services as separate entities. The domain/object model provides explicit representation of key objects, and key service and network performance metrics.

WO 01/091369 A3

INTERNATIONAL SEARCH REPORT

	onal Application No
	PCT/CA 01/00725

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/26 H04L12/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 061 724 A (MATHIEU LOIC ET AL) 9 May 2000 (2000-05-09) abstract	1-9, 11-13
Y	column 2, line 62 -column 4, line 7 column 5, line 48 -column 7, line 40 column 10, line 17 - line 32	10,14

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents:

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 March 2002	27/03/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Stergiou, C

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 01/00725

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	PAVLOU G ET AL: "INTELLIGENT REMOTE MONITORING" BRINGING TELECOMMUNICATION SERVICES TO THE PEOPLE - ISS & N 1995. THIRD INTERNATIONAL CONFERENCE ON INTELLIGENCE IN BROADBAND SERVICES AND NETWORKS, HERAKLION, CRETE, OCT. 16 - 19, 1995. PROCEEDINGS, PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INT, vol. CONF. 3, 16 October 1995 (1995-10-16), pages 430-444, XP000593493 ISBN: 3-540-60479-0	10,14
A	abstract page 430, line 1 -page 435, line 3 page 442, line 6 - line 22	1-9, 11-13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Ir tional Application No
PCT/CA 01/00725

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6061724 A	09-05-2000	FR 2758896 A1	31-07-1998
		AT 206831 T	15-10-2001
		DE 69801984 D1	15-11-2001
		EP 0954788 A1	10-11-1999
		WO 9833123 A1	30-07-1998